What is claimed is:

1. A system for decrypting an encrypted computer program, comprising:

means for generating a first cipher key from a first block of the encrypted computer program;

means for decrypting a plurality of second blocks of the encrypted computer program with said first cipher key;

means for generating a second cipher key from one of said plurality of second blocks; and

means for decrypting another of said plurality of second blocks with said second cipher key.

2. The system as set forth in claim 1,

wherein said first block is not encrypted.

3. The system as set forth in claim 1,

wherein said plurality of second blocks are encrypted at least with said first cipher key before treaded by this system.

4. The system as set forth in claim 3,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key before treated by this system.

5. The system as set forth in claim 1, further comprising:

means for detecting whether or not the encrypted computer program is analyzed; and

means for decrypting a plurality of dummy blocks instead of said plurality of second blocks if it is detected that the encrypted computer program is analyzed.

6. A method for decrypting an encrypted computer program, comprising the steps of:

generating a first cipher key from a first block of the encrypted computer program;

decrypting a plurality of second blocks of the encrypted computer program with said first cipher key;

generating a second cipher key from one of said plurality of second blocks; and

decrypting another of said plurality of second blocks with said second cipher key.

7. The method as set forth in claim 6,

wherein said first block is not encrypted.

8. The method as set forth in claim 6,

wherein said plurality of second blocks are encrypted at least with said first cipher key before treaded by this method .

9. The method as set forth in claim 8,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key before treated by this method.

10. The method as set forth in claim 6, further comprising the steps of:

detecting whether or not the encrypted computer program is analyzed; and decrypting a plurality of dummy blocks instead of said plurality of second blocks if it is detected that the encrypted computer program is analyzed.

11. A computer program product embodied on a computer-readable medium and comprising code that, when executed, causes a computer to perform a method for decrypting an encrypted computer program, said method comprising the steps of:

generating a first cipher key from a first block of the encrypted computer program;

decrypting a plurality of second blocks of the encrypted computer program with said first cipher key;

generating a second cipher key from one of said plurality of second blocks; and

decrypting another of said plurality of second blocks with said second cipher key.

12. The computer program product as set forth in claim 11,

wherein said first block is not encrypted.

13. The computer program product as set forth in claim 11,

wherein said plurality of second blocks are encrypted at least with said first cipher key before treaded by this method .

14. The computer program product as set forth in claim 13,

wherein at least one of said plurality of second blocks is encrypted with said second cipher key before treated by this method.

15. The computer program product as set forth in claim 11, wherein said method further comprises the steps of:

detecting whether or not the encrypted computer program is analyzed; and

decrypting a plurality of dummy blocks instead of said plurality of second blocks if it is detected that the encrypted computer program is analyzed.

16. A data structure embodied on a computer-readable medium comprising:

a non-encrypted block; and

a plurality of encrypted blocks;

wherein said plurality of encrypted blocks are encrypted with a cipher key generated from said non-encrypted block, and

wherein one of said plurality of encrypted blocks is encrypted with a cipher key generated from another of said plurality of encrypted blocks.